The U.S. General Services Administration is seeking comments by close of business on 6/23/00 on the attached Draft Request For Proposals for the proposed requirement to acquire support for the Federal Intrusion Detection Network-FIDNet-which will consist of hardware, software, and supporting services and facilities to analyze intrusion alerts from participating Federal agencies' intrusion detection systems. This notice requests comments or expressions of interest only, to be emailed to Mr. Arnold G. Eugene at arnold.eugene@gsa.gov, or send hard copies to GSA-FTS-OIS, Attn: Arnold Eugene, Room 5060, 7th and D Sts., SW, Washington, DC 20407. Do not send proposals at this time.

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 Specification

The contractor shall supply all personnel, materials and services necessary to perform the requirements set forth in this contract.

B.2 Prices all Inclusive

Any equipment, material, facility, site preparation or service required in the performance of this contract in which prices have not been specifically identified by the Offeror, will be considered to be included in the total price of this contract or be provided at no additional cost to the Government during the life of this contract, unless otherwise specified in the contract.

B.3 Solicitation/Contract Item Numbers and Service Requirements

The solicitation/contract item numbers and service requirements are described as follows (all items include the customer as part of the data correlation/mining effort, as well as the attack information dispersal process):

01 – Standard Service: Monitor intrusion detection sensor(s) output, provide analysis and response.

02 – Plus Service: Monitor intrusion detection sensor(s) output, provide analysis and response, provide reports (see C.6).

03 – Full Service: Monitor intrusion detection sensor output, provide reports, and manage security devices for the customer.

B.4 Cost or Pricing Information

Offerors are required to submit cost or pricing information in order to support the Offeror's Estimated Total Prices (Section B, Price Schedules) for each service offered. Cost or pricing information should include the following:

1. Description of services offered.
2. Non Recurring unit prices for offered services
3. Monthly recurring unit prices for offered services
4. Other pertinent information to support cost or pricing.

B.5 Instructions for Preparing the Section B Price Schedule:

a. Provide the Unit NRC for each line item under the Base Year.

b. Provide the Unit MRC for each line item under the Base Year.

c. Calculate the Extended NRC by multiplying the government estimated quantities by the unit NRC.

d. Calculate the Extended MRC by multiplying the government estimated quantities by the unit MRC.

e. Calculate the total price by adding the results of c and d above.

f. Calculate each year's total price subtotal by summing the Total Price column for each year and multiply it by 12 months.

g. Calculate the total contract price by adding the subtotals for the Base year and each of the 4 option years.

Price Table							
Unit price is on a per monitored device basis.							
Offeror may show volume price breaks if applicable by duplicating this spreadsheet and labeling each sheet appropriately.							
NRC = Non-Recurring Charge							
MRC = Monthly Recurring Charge							
Base Year							
		Estimated	**Unit Price**		**Extended Price**		

Item	Description	Quantity	NRC	MRC	NRC	MRC	Total Price
01	Standard Service	50					
02	Plus Service	100					
03	Full Service	25					
Subtotal:							
Option Years							
Year One							
		Estimated	**Unit Price**		**Extended Price**		
Item	**Description**	**Quantity**	**NRC**	**MRC**	**NRC**	**MRC**	**Total Price**
01	Standard Service	100					
02	Plus Service	200					
03	Full Service	50					
Subtotal:							
Year Two							
		Estimated	**Unit Price**		**Extended Price**		
Item	**Description**	**Quantity**	**NRC**	**MRC**	**NRC**	**MRC**	**Total Price**
01	Standard Service	150					
02	Plus Service	300					
03	Full Service	75					
Subtotal:							
Year Three							
		Estimated	**Unit Price**		**Extended Price**		
Item	**Description**	**Quantity**	**NRC**	**MRC**	**NRC**	**MRC**	**Total Price**
01	Standard Service	203					
02	Plus Service	405					
03	Full Service	101					
Subtotal:							
Year Four							
		Estimated	**Unit Price**		**Extended Price**		
Item	**Description**	**Quantity**	**NRC**	**MRC**	**NRC**	**MRC**	**Total Price**

01	Standard Service	253					
02	Plus Service	506					
03	Full Service	127					
Subtotal:							
Total Contract Price:							

Section C
Descriptions/Specifications/Work Statement

C.1 Background

OMB Circular A-130:

OMB Circular A-130, Appendix III establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems. The appendix also instructs the General Services Administration (GSA) to "provide appropriate security services to meet the needs of Federal agencies" and to develop "contract vehicles for agencies to use in the acquisition of cost-effective security products and services." FIDNet will be just such a vehicle.

In accordance with the circular, "agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM)."

Presidential Decision Directive-63[1]:

Additionally, Presidential Decision Directive-63 (PDD-63) and the associated *National Plan for Information Systems Protection, Version 1.0* call upon the US Government to set an example for the nation in securing its critical information infrastructure. The federal critical information infrastructure includes, for example: publicly accessible networks, operated by the Defense Department to sustain its global presence; networks linking the air traffic control system to the thousands of aircraft in flight daily; networks linking federal finance and trade entities with counterparts in the business world; and networks providing benefits to and receiving revenues from the American public. The availability of these critical national computing and communications capabilities is essential to the national defense, economic well-being, and social welfare of the United States, and our reliance on them is growing.

To address the growing risk created by the federal government's increasing reliance on networked computers and the diverse and escalating threats here and abroad, the federal government will develop a capability that reduces the risk of an unidentified, successful intrusion

[1] Presidential Decision Directive #63, "Critical Infrastructure Protection," May 22, 1998.

into critical federal computing networks and systems. This capability will enable systems administrators, agencies, departments, and the federal civilian government as a whole to act in a more coordinated manner in detecting, assessing, deterring, protecting, and responding to attacks on the critical information infrastructure at both the local and national levels. In short, it will improve computer security across agencies and in the process will provide the federal civilian government its first integrated line of defense against computer intrusions.

C.1.1 FIDNet Defined

FIDNet is an aggregate solution inclusive of all hardware, software, services and supporting facilities to receive and heuristically analyze the alerts and notifications from participating agencies' indigenous intrusion detection systems. Its purpose is to enhance the civilian Federal Government's overall information security posture with respect to computer intrusions. When an event is identified, FIDNet shall be primarily concerned with information sharing among subscribers to include protocol or procedures to preclude similar intrusions at other agencies. A graphical depiction of FIDNet's concept of operations is shown in figure C.1.1 below.

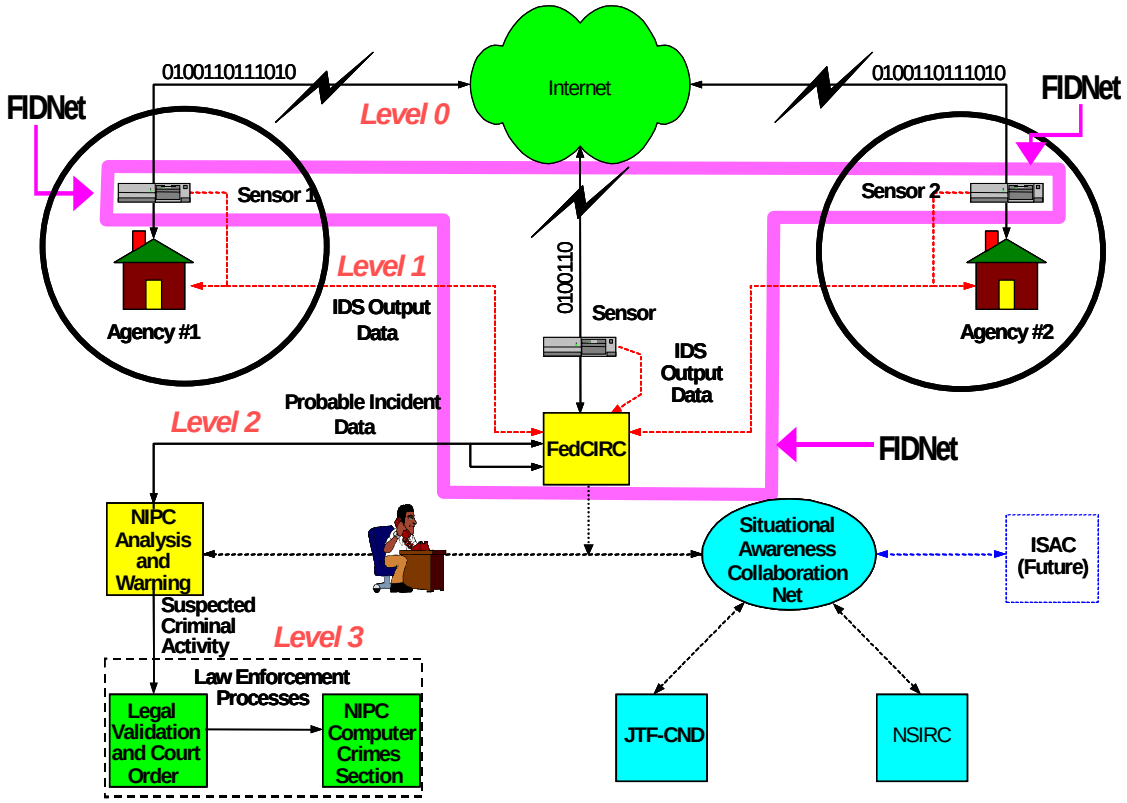

Figure C.1.1 Depiction of FIDNet Concept of Operation

C.2 Scope - General

The government plans to award a multiple Indefinite Delivery/Indefinite Quantity contract for one (1) year with four (4) one-year options, which will provide for this security service. If a multiple award is made, the awardees shall be responsible for meeting all the requirements specified in this Section C collectively just as they would have been required to do individually. The solution shall be fully integrated. The government reserves the right to make a single award if it is determined that it is the best interest of the government.

The Federal Intrusion Detection Network will be a (global) collaborative decision environment that will support and enhance the development, analysis, selection and rapid execution of FedCIRC courses of action within the federal government's threat-reaction cycle. The successful offeror shall correlate/fuse intrusion, vulnerability, and event data with other intelligence and operational data to facilitate attack characterization, attribution and prevention.

Services provided will be either for the Federal Computer Incident Response Capability (FedCIRC) directly or for other federal agencies for which FedCIRC is acting as an agent under a Memorandum of Understanding (MOU). The successful offeror shall design, implement, and maintain the capability, inclusive of facilities, hardware, software and service personnel, to provide FIDNet service as defined in this Section C.

C.3 Services Required

Proposed FIDNet solutions shall enhance existing FedCIRC security operations capability. Upon award, the successful offeror shall immediately assess all factors necessary to size the hardware, software and support requirements for the infrastructure solution being offered for initial operations. This prototype capability shall be available for operation within 90 days of contract award.

As additional agencies execute MOUs with FedCIRC to subscribe to FIDNet, the successful offeror will propose additionally required quantities as necessary to support the increased requirements. The government will evaluate proposed increases to order quantities and reserves the right to negotiate the quantities.

Once on line with FIDNet, the participating agencies' ID system(s) output(s) shall be received and reviewed by contractor-provided expert network security specialists and systems. Analysis, response, and communication functions shall be performed. Further, the successful offeror shall develop a procedure for effectively communicating analysis results, test plans, attack signatures, and all other critical information to all participating agency members and FedCIRC. Such communication will be designed to address the data needs of both the technician and management.

It is anticipated that in order to achieve the requirements, the successful offeror shall provide a variety of services that may include, but are not limited to:

(a) Multi-Vendor IDS Analysis Capability

(b) Expert Observation, Analysis, and Response for Network Security

(c) FIDNet-wide correlation and data mining

(d) Automated attack identification and response systems

(e) Facilities Support

(f) Training

C.3.1 Management and Operations

C.3.1.1 Problem Identification and Resolution

The successful offeror shall implement and maintain a system for receiving, recording, responding to, and reporting FIDNet problems within its own organization and to the government.

C.3.1.2 Customer Service Records

The successful offeror shall implement and maintain a system of records relating to customer requests for services and the services provided.

C.3.1.3 Physical Security Controls

The successful offeror shall implement appropriate physical security controls to restrict access to hardware and to be used in connection with providing FIDNet services. Such access controls shall be monitored for unauthorized intrusion at all times.

C.3.2 Promotion of FIDNet

FIDNet contractors shall actively promote the FIDNet program, products, and services. FIDNet promotion plans for initial and ongoing performance during the period of the contract shall be proposed

.Promotion materials that contain any and all references to FIDNet shall not:

(a) Interpret contract terms or conditions

(b) Use Government official seals and logos unless otherwise agreed upon in writing by the GSA Procuring Contracting Officer (PCO).

All promotion materials that contain any references to FIDNet shall be submitted to GSA for written approval prior to use. All such materials will be reviewed for content and adherence to specifications (a) and (b) above and written approval/disapproval will be issued within 7 calendar days of receipt. Revisions shall be submitted to allow sufficient time for review.

C.4 Standards and Operating Environment

C.4.1 Intrusion Detection Systems (IDS) Supported

As a minimum FIDNet shall be able to support/interface with the following IDS packages:

ISS	CyberSafe	NAI/PGP	NID
Raytheon	Intrusion.com	Axent	
Cisco	Etrust	NFR	

Note: As the market and the industry move toward an accepted standard for IDS, this partial enumeration will be superseded by a requirement simply to support any IDS which meets the NIST-approved standard.

C.4.2 Internet Communication and Standards

Compliance with the latest versions of the Internet Engineering Task Force (IETF), specifically those of the IETF's Intrusion Detection Working Group, and World Wide Web Consortium (W3C) standards is required throughout the duration of the contract. FIDNet contractors shall ensure continuing conformity with evolving standards as they impact this contract, at no additional cost to the Government.

C.4.3 Date/Time Stamp

Where applicable, FIDNet date/time stamps shall conform to the ITU-T Recommendation C.690 and X.690 v2, “Information Technology – ASN.1 Encoding Rules,” 1994. FIDNet contractors shall use Coordinated Universal Time (UTC) NIST as the reference time base. FIDNet contractor’s time shall be synchronized within one second and granularity of time expressed shall be at least to the granularity of one minute.

C.4.4 IDS to FIDNet Communications

IDS output data being fed from agency IDS' to FIDNet shall be secure. The contractor shall detail how this will be accomplished. As a minimum, authentication, encryption, and protocols shall be addressed.

C.4.5 Capture of Forensic Evidence

The FIDNet solution shall be capable of capturing forensic evidence when a multi-site or multi-subscriber event is detected, *i.e.*, an event unique to FIDNet which will not have already been reported by the subscribing agency through its normal channels. This retained information shall meet or exceed all legal requirements for criminal prosecution in accordance with federal law.

C.4.6 Scalability

The performance of FIDNet systems and services shall not suffer due to the following variances:

(a) Traffic volume (surges)

(b) Types of sensors

(c) Quantity of sensors

(d) Changing network topologies within subscribing agencies

C.5 Performance

C.5.1 Hours of Operation

FIDNet contractors shall operate 24 hours per day, seven days per week, including Federal holidays.

C.5.2 Availability/Reliability

All services and products specified shall, at a minimum, be fully operational and available for use no less than 99.5 percent of the time. There shall be no scheduled downtime without written approval from the ACO and COTR.

C.5.3 Response Time for Services

IDS output data shall be monitored and analyzed real-time during the entire performance period. The successful offeror shall demonstrate the capability to disseminate critical information stemming from an attack to all FIDNet subscribers within 15 minutes of identifying the attack. This information shall provide customer network engineers methods to avoid/recover from such an attack.

FIDNet contractors shall implement specified services according to the response times set forth Section F.

C.6 Reporting Requirements

The successful offeror shall provide all results of studies and analyses as described throughout the preceding paragraphs in electronic formats. Reports shall be designed to allow measurement of FIDNet program effectiveness in identifying, analyzing, and responding to unauthorized access and use of government systems. These reports shall be available on a per-customer, as well as a FIDNet-wide basis. Technical response to this requirement shall describe proposed reporting capability in detail.

More specific reporting requirements are stated in Section G to be used for administering the contract. These reports will be provided at no additional charge to the government.

This portion of Section L is meant as an example of what might be included in the RFP. The omission of some sections is to allow focus on the subjects previously discussed in FIDNet meetings.

L.9 Subcontract Plan

(a) Large business offerors shall submit a subcontracting plan in the Volume IV - Contract and Associated Data. The plan must be submitted in accordance with FAR Parts 19, with specific attention paid to FAR 19.704, FAR 52.219-9.

(b) All cost and technical information must be included in the appropriated sections of the offeror's proposal in addition to submission of the subcontracting plan.

(c) The offeror shall show the subcontractor's business size, the percentage and type of workload estimated to be subcontracted out.

(d) All prospective subcontractors contacted by your firm in any manner should be expressly advised in writing that no solicitation on your behalf shall be construed in any manner to be an obligation on your part to enter into a subcontract with said subcontractor. Nor shall any contract result in any claim whatsoever against the United States Government for reimbursement of costs for any efforts expended by said subcontractor, regardless of whether or not your firm is successful in receiving a contract as a result of this proposal.

(e) The subcontracting plan goals for this acquisition are as follows:

Small Disadvantaged Businesses	=	6% of the total contract price
Women-Owned Small Businesses	=	4% of the total Contract price
Small Businesses	=	10% of the total contract price
Total	=	20% of the total contract price

(f) The prime contractor shall submit on an annual basis a list of the current subcontractors on their contract.

L.10 RESERVED

L.11 RESERVED

L.12 Security Requirements

(a) The DD-254, DOD Contract Security Classification Specification, requires the contractor to have or be able to obtain the security clearances specified for performance under this contract. At contract award, contractors shall have required clearances necessary to perform the requirement.

(b) Offerors shall demonstrate that they either currently have the required clearances or interim clearances upon contract award.

L.13 Prime Contractor Responsibilities

In the conduct of individual orders contractors are encouraged to subcontract and/or enter into multiple teaming arrangements with small, small disadvantaged, women-owned, and Hubzone Small Businesses, as described in FAR Part 19. However, the Prime Contractor shall bear total responsibility for the performance of all obligations under any contract awarded from this solicitation.

L.14 Acceptance of Proposals

The Government reserves the following rights:

(a) To consider as acceptable only those proposals that are submitted in accordance with all technical requirements stated or referenced in the solicitation and that demonstrate an understanding of and the ability to perform the Government's requirements; and

(b) To reject as unacceptable those proposals that delete or alter technical requirements of the solicitation.

L.15 Submission of Proposals

Due date/time: The offer shall be delivered to the address shown in paragraph L-16(f)(2) by the time and date specified on the SF 33, block 9. Offers received after the time and date specified shall be considered late.

L.16 Instructions for Preparation of Proposals

(a) Purpose: These instructions prescribe the proposals format. They are designed to ensure the submission of information essential to the understanding and comprehensive evaluation of proposals. Offerors are cautioned to follow the instructions carefully. THE GOVERNMENT RESERVES THE RIGHT TO REJECT ANY PROPOSAL THAT DOES NOT COMPLY WITH THE PROPOSAL PREPARATION INSTRUCTIONS.

(b) Proposal Format: Offerors shall submit their proposal in electronic format, in accordance with the following instructions. All word processing and spreadsheet documents shall be provided in MS Office 97. For written documents - MS Word, for presentations - MS PowerPoint, for spreadsheets - MS Excel. Landscape pages shall face right. Font shall be Arial 11 Point.

(c) Page Numbering: Each offeror shall use a standard page numbering system to facilitate proposal references. Number consecutive pages within sections. Charts and figures should be numbered as part of the page numbering system.

(d) Page Limitations. Page limitations are identified with the associated submission requirement in Paragraph L-17 below, and shall be treated as maximums. If exceeded, the excess pages will not be read or considered in the evaluation of the proposal and will be returned to the offeror as soon as practicable. When both sides of a sheet display printed material, it shall be counted as 2 pages. Foldouts shall be counted as 2 pages. Included in the page count are separate pages providing graphics, charts, illustrations and pictures.

(e) Cost/Price Data: No cost or price data of any kind shall be included in any volume except Volume III.

(f) Submission Of Proposal:

1. In accordance with FAR 52-215-1, a complete proposal submission shall be considered provided when all volumes are received by the Procuring Contracting Officer named elsewhere in this document.

2. The electronic proposal, by volume, shall be furnished to web address: https://www.fidnetsubmittal.fedcirc.gov

In order to respond to this solicitation over the world wide web, users must obtain a certificate from an Interim External Certificate Authority (IECA). This certificate will allow the FedCIRC web site to verify the identity of the responder. The list of currently approved IECAs, and links to their web sites, is available at _____.

To obtain an IECA certificate, it will be necessary to use a web browser with 128-bit (domestic strength) encryption. A recent version of the web browser is recommended, either Netscape 4.7, available from http://home.netscape.com/computing/download/index.html or Internet Explorer 5.01, available from http://www.microsoft.com/downloads/default.asp. As part of the certificate enrollment process, users will need to verify their identity with a representative of the IECA or a notary public. It should take about three to four days to obtain the certificate.

Vendors may submit their proposal at: https://www.fidnetsubmittal.fedcirc.gov using the web browser that was used to obtain the IECA certificate. They will be prompted to select their certificate by the browser during the submission process. The web session will be protected by Secure Sockets Layer (SSL), ensuring both the confidentiality of the submission as well as secure authentication of the vendor.

Testing by the vendors to ensure that they can upload their proposals can be done the week of July 10, 2000. Point of contact at FIDNet if you have questions concerning testing or for proposal submission is Arnold Eugene at 202-401-3485.

Separate the electronic files of the proposal by Volume. Each file must be autonomous and complete. Perform a virus check prior to proposal submittal. Virus checking will be conducted at the source selection site prior to the beginning of the evaluation using the current version of Norton Anti-Virus. In addition to electronic submission, each proposal shall be submitted in CD-ROM format. All proposal information/submissions must be received by the closing date and time specified on the SF33.

Upon approval by the government, all awardees will have the opportunity to provide a web-page link for display on the FedCIRC web site. This page will provide additional information on the products and services available as part of this contract. More information will be available at contract award.

L.17 Instructions for Preparation of Proposals – Content

(a) Executive Summary - 2 Page Limit

The offeror shall provide a 2-page executive summary that describes the significant attributes of their proposal.

(b) Volume I Technical Proposal.

The offeror's technical proposal shall address all aspects of the statement of work, Section C of this solicitation. Each portion of Section C shall be addressed under its own tab in the technical proposal Volume I. A Table of Contents shall be included to allow quick reference to each section of the proposal. The page number limitation is 50. The government strongly discourages the inclusion of information (i.e. Generic sales and marketing literature) that does not directly relate to the technical specifications of this solicitation.

In responding to Section C, the offeror must address the following critical points:

1. The means of secure communications between the originating sensors, the analysis cell, and FedCIRC

2. The nature and design of the correlation engine

3. Data storage requirements

4. An approximation of received data's useful life, *i.e.*, the period of time after which the engine will no longer consider data to be relevant and the protocol to expunge the expired data

5. An estimate of the numbers of both government and contractor personnel required to man/operate the associated operations center. Identify whether this ops center should be operated by the government or by the contractor.

6. An estimate of the system's physical presence in the security operations center (whether government or contractor-operated), at FedCIRC and on subscribers' premises, *i.e.*, how large a footprint is anticipated at each location

7. An assessment of scalability, *i.e.*, how the proposed system will be designed to handle new FIDNet subscribers as they execute MOUs with FedCIRC

8. An enumeration of the specific IDSs to be supported
   [NOTE: These may include commercial off-the-shelf (COTS), government off-the-shelf (GOTS) or other intrusion detection offerings]

9. The method for providing FedCIRC visibility of activity pertaining to any FIDNet-affiliated subscribers

10. Whether or not the solution includes or will include non-FIDNet subscribers

11. The method, if any, of segregating FIDNet-affiliated subscribers from others

12. Any prerequisites for subscribers (FIDNet-affiliated or otherwise)

(c) Volume II - Past Performance

The offeror shall identify four recent (completed within last 3 years, 1998-2000, or ongoing) contracts or task orders which they performed as the prime contractor for evaluation by the Government team. In selecting the four contracts or tasks orders, offerors should consider the factors stated in Section M, as well as the technical areas identified in the statement of work. Accuracy of past performance data is critical, as the Government will verify the information provided for each effort.

As it pertains to each of the four identified past performance efforts, provide the following:

1. Identify the key requirements of the statement of work. Include information on the size, scope and complexity of the requirement. Include the performance requirements and any Government identified performance metrics/requirements.

2. Identify significant obstacles or technical challenges to achieving the required performance and solution. Identify innovative technical approaches or solutions that helped achieve the required performance.

3. Identify the key aspects of the offerors' program management and quality control program. Identify the management tools and techniques that were applied to the identified past performance efforts.

4. Detail the results of the application of the offeror's quality control and management program. Provide performance standards, and actual results achieved on the identified program. (*e.g.*, cost, schedule, and performance baseline and actual performance results.)

5. Provide organizational charts identifying the size, scope and structure of the offeror's Information Security organization. Indicate the date the organization was established. If a matrix organization, only identify the resources directly assigned to the organization.

6. Identify individuals and provide resumes - 2 page limit (address the person's education and experience with regard to the position proposed) for the Key Personnel to be identified in H-9(D). If any proposed key personnel are not currently employed with the offeror, the offeror shall submit letters of commitment along with the person's resume. (Letter of Commitment does not count against the 2 page limitation)

7. Complete a resource matrix form that identifies the number of personnel directly assigned to the organization that will be responsible for performing the contract, the labor category and title of all assigned personnel, and level of security clearance for each assigned individual.

8. Address, in detail, the ability to recruit, train, maintain, and retain high quality personnel. Following the direction of FAR 52.222-46, Offerors shall provide a "Compensation for Professional Employees Plan" for evaluation.

(d) Volume III -- Cost/Price Proposal.

1. The Cost/Price Proposal Volume shall include prices for Section B. The offeror shall comply with the instructions for development of its cost/price proposal outlined in Section B, and L-15 and L-16, above. The offeror shall submit information other than cost or pricing data in support of the prices proposed. The proposal for Section B shall include the cost breakdown for the Labor Rates, the mark-up rate that is applied to ODCs, and a proposed profit for the firm, fixed-price ODCs. Offerors will furnish prices for the Base Period and all Option Periods, in the Section B Schedule format. Prime contractors are limited to first-tier subcontractors only; no second-tier, third-tier or any other tier subcontractors are allowed. All labor will be reimbursed via the proposed time-and-material and firm, fixed-price composite rates. Cost Reimbursable may be negotiated on a case-by-case basis, but will not be evaluated for award purposes.

2. The use of uncompensated overtime is not allowed. The offerors shall propose all hourly rates based on a 40-hour work-week (2080 hours per year).

3. An offeror's proposal is presumed to represent its best efforts to respond to the solicitation. Any inconsistency between promised performance, the Technical Proposal, identified personnel resources, and cost/price must be explained in the proposal. For example, if the intended use of new and innovative techniques is the basis for an abnormally low estimate, the nature of these techniques and their impact on cost or price shall be explained; or, if a corporate policy decision has been made to absorb a portion of the estimated cost, that must be stated in the proposal. Any inconsistency, if unexplained, may raise a fundamental question of the offeror's understanding of the nature and scope of the work required and may adversely impact the offeror's standing upon evaluation. The burden of proof as to cost credibility rests with the offeror. Unrealistically low prices may indicate an inability to understand requirements and a high-risk approach to contract performance. Accordingly, the Government may

consider the findings of such an analysis in evaluating an offeror's ability to perform and the risk of its approach.

4. The prime contractor shall forward one (1) complete copy of its pricing proposal to its applicable DCAA office. This will save time in verifying rates with the various DCAA offices. Information on each burden/indirect cost rate shall be furnished for each burden center, *i.e.*, G/A, facilities capital cost of money, fringe, engineering overhead, profit, etc. The prime contractor shall explain how the proposed composite rate was developed.

5. Subcontractors will not be required initially to submit information other than cost or pricing data in support of the prices proposed. However, the Government reserves the right to request this information if needed to determine price reasonableness.

6. Offerors shall submit their proposal via electronic submission (L-16f2) and a copy on CD-ROM, using Microsoft Office 97, i.e., Microsoft EXCEL Version 5.0 or Microsoft EXCEL 97 software. Prospective offerors shall submit Discounted Life Cycle Cost (DLCC) based strictly upon criteria established in Section M incorporating proposed prices in Section B. This approach will serve to disclose any potential proposal ambiguities or misinterpretations and will help ensure a mutual understanding of the pricing methods proposed. The offeror's DLCC calculations will be used only to assess potential problems or discussion areas. Price proposals not including all options shall not be considered for award. NO SUBSTITUTE PRICING SUMMARIES (SECTION B) ARE ACCEPTABLE.

(e) Volume IV - Contract and Associated Information.

The offeror shall submit the following within Volume IV.

Tab A Transmittal Letter and Standard Form 33.
Tab B Section K Representations and Certifications
Tab C EEO Pre-award Clearance Information
Tab D Demonstration Material.
Tab E Subcontracting Plan (Large Business Only)

1. Tab A: Transmittal Letter and Standard Form 33.

a. Section 1. Transmittal Letter

Offerors shall submit a cover letter transmitting the proposal. The cover letter shall address the information required by FAR 52-215.1(c)(2). 2 Page Limit

b. Section 2. Standard Form 33 (SF 33).

The offeror shall include a completed SF 33 properly executed and signed by an official authorized to commit the offeror. Acknowledgment of receipt of amendments may be made in either the transmittal letter of block 14 of the SF 33.

2. Tab B: Section K Representations and Certifications

The offeror shall submit properly executed representation and certifications identified in Section K, Representations, Certifications, and Other Statements of Offerors of the RFP.

3. Tab C: EEO Pre-award Clearance Information

To expedite the Government's EEO Pre-award Clearance Request process, the prime contractor shall include a list of all proposed subcontractors with a proposed subcontract value estimated at $10 million or more, to include the following information: Name, address, individual's name/point of contact, and telephone number. The Government plans to request EEO Clearance early in the evaluation process to avoid possible delays in making contract award.

4. Tab D: Demo Material

The offeror shall include all materials they anticipate presenting at the demos in Tab D.

5. TAB E: Subcontracting Plan

The offeror shall submit a subcontracting plan that addresses the requirements of FAR, with specific attention paid to FAR 19.704, FAR 52.219-9. The plan shall identify key aspects of how the offeror plans to meet or exceed the small business subcontracting goals of this solicitation.

L.18 Capability Demonstrations (Demos)

(a) General Information.

The Government intends to award contracts based on initial proposals, and without conducting discussions. As such, the scope and content of exchanges that may occur between the Government's participants and the offeror's representatives is limited to clarifications.

(b) Purpose Demos.

The purpose of demonstrations is to show the government capabilities and interfaces that might not be ostensible in the written proposal. The offeror should take this opportunity to demonstrate their product's ability to meet as many requirements specified in Section C as reasonable.

(c) Demo Time.

Offeror demos are planned for 90 minutes. At the conclusion of the demonstration, the Government plans 30 minutes for a Question and Answer period. The offeror may not exceed the 90 minute time limit. However, if required, the Government reserves the right to exceed the planned 30 minute question and answer session.

(d) Demonstration Scheduling.

1. The Contracting Officer will schedule demos by assigning dates at random. Offerors will be notified of its demo date at least 20 days prior.

2. The first demo and Q&A session will take place approximately 30 days after receipt of proposals.

3. The contracting officer may approve the rescheduling of demos for good cause. However, offerors are expected to arrange their schedules, and the schedules of any key personnel to enable dates to be met. Avoidable schedule conflicts (*e.g.*, previously scheduled vacation or other business commitments) are not considered good cause.

(e) Demonstration Location.

The government's preference is for all demos to take place in the Washington DC area. The offeror may make a case for an alternate location if it significantly raises the value of the demonstration.

(f) Demonstration Attendance.

1. Representation of the offeror at the demo and Q&A sessions is limited to the key personnel identified in the proposal. These key personnel will perform the demonstration and answer questions at the Q&A session. Therefore, an offeror must ensure that the key personnel will be able to address all aspects of their proposal.

2. As many as three additional people may attend. (Note: It is anticipated that these same individuals will attend any post-award debriefing.)

(g) Demonstration Equipment

Offerors shall be responsible for providing all necessary equipment.

(h) Demonstration Topics.

In demonstrating, offerors are strongly encouraged to take into consideration the relative order of importance for Section M evaluation criteria in planning their demo.

SECTION M Evaluation Factors for Award

CLAUSES INCORPORATED BY REFERENCE:

52.216-27
Single or Multiple Awards
OCT 1995

PART IV REPRESENTATIONS AND INSTRUCTIONS
SECTION M
EVALUATION FACTORS FOR AWARD

M.1 Evaluation Process

(a) The Government intends to conduct source selection in accordance with the competitive negotiated source selection procedures contained in Federal Acquisition Regulation (FAR), Part 15. The Government anticipates award based on initial proposals and does not plan to conduct discussions.

(b) The Government will evaluate initial proposals in accordance with M-3. Based on the ratings of each proposal against all evaluation criteria, the Government will identify the most highly rated proposals. The Government intends to allow each Offeror an opportunity to participate in capability demonstrations. However, the Government reserves the right to conduct a "voluntary down-select", whereby, prior to scheduling demonstrations, the Government will give Offerors whose proposals do not appear to have a reasonable chance for award, the opportunity to decide whether they want to proceed with the competition. The Offeror must make the business decision as to whether to continue in the competition.

(c) In accordance with FAR 15.306(a), Offerors may be given the opportunity to clarify certain aspects of this proposal or to resolve minor or clerical errors. This includes capability demonstrations.

M.2 BASIS FOR AWARD

(a) This will be a full and open procurement.

(b) The Government intends to make multiple Indefinite Delivery/Indefinite Quantity awards to the highest rated proposals representing the best value in accordance with the evaluation criteria identified in this solicitation. Awardees shall collectively provide the requirements specified in Section C. The solution shall be fully integrated. The government reserves the right to make a single award if it is determined that it is the best interest of the government.

(c) In accordance with FAR 52-215-1(f), the Government intends to award a contract or contracts resulting from this solicitation to the responsible offeror(s) whose proposal(s) represents the best value after evaluation in accordance with the factors and subfactors in the solicitation. The Government intends to evaluate proposals and award a contract without discussions with offerors (except clarifications as described in FAR 15.306(a). Therefore, the offerors' initial proposal should contain the offerors' best terms from a cost/price and technical standpoint. The Government reserves the right to conduct discussions if the Contracting Officer later determines them to be necessary.

(d) The contract award decision will be determined based on the Government's evaluation of each offeror's complete proposal against the evaluation criteria identified in paragraph M-3 below. Awards will be made to offerors whose proposals contain the combination of factors offering the best overall value to the Government. Best value means the expected outcome of an acquisition that, in the Government's estimation, provides the greatest overall **benefit** in response to the requirement (FAR 2.101). In making this evaluation, the Government is more concerned with obtaining superior product, management and technical skills than with making an award to the offeror with the lowest price(s).

(e) When conducting the evaluation, the Government may use data included by offerors in both their proposals and in the demonstrations, as well as data obtained from other sources. While the Government may elect to consider data obtained from other sources, each offeror is responsible for ensuring that the information provided is thorough and complete.

M.3 Evaluation Criteria

(a) General: The Government will apply the following tailored evaluation criteria to identify the best value proposal(s). The evaluation criteria represent key areas of importance to be considered in the source selection decision. The factors and sub-factors were chosen to support meaningful comparison and discrimination between and among competing proposals.

(b) Legal: Any proposal recommended for award will be submitted to the Department of Justice for legal review. The Department of Justice will ensure the proposed solution fully complies with the Electronic Communications Privacy Act (ECPA), the Privacy Act of 1974, the Freedom of Information Act (FOIA), the Inspector General Act of 1978, and all applicable laws and regulations as they pertain to this contract. No award shall be made which does not pass this review.

(c) Relative Importance: Technical Solution (Non-Price Factor 1) is significantly more important than Past Performance (Non-Price Factor 2). Each Non-Price Factor individually is more important than Cost/Price. When combined, Technical Solution and Past Performance are significantly more important than price.

(d) Non Price Factors

1. Factor 1: Technical Solution
The government will evaluate the technical response to Section C of this solicitation to determine understanding of the requirements and their solution. The government will evaluate the overall technical strength of the proposal and how well it fits the definition of FIDNet (Section C). Subfactors are listed in terms of relative importance

a. Sub Factor 1, Technical Solution: Multi-Vendor Support
The government will evaluate the approach, and to what degree the solution offered integrates with existing intrusion detection systems, firewalls, and proxies. The solution's adherence to existing standards, as well as its ability to seamlessly adopt evolving standards is a prime consideration.

b. Sub Factor 2, Technical Solution: Automated Analysis and Response Capability
The government will evaluate the solutions' ability to provide a FIDNet-wide correlation and analysis engine. Emphasis will be placed on its effectiveness in raising the intrusion detection and response capabilities both of FIDNet subscribers and of the government as a whole. Elegance, scalability, survivability, strength, and internal security of the solution will be thoroughly examined for both single and multi contractor scenarios.

c. Sub Factor 3, Technical Solution: Information Dissemination Efficiency
The government will evaluate the proposed methodology of disseminating intrusion identification and response information to FIDNet subscribers and FedCIRC. Elegance, scalability, survivability, technical strength, internal security of the solution will be thoroughly examined for both single and multi contractor scenarios.

The government may take into consideration additional features or capabilities over and above specified requirements if they are determined to improve on the core requirements for FIDNet. Features and capabilities outside the scope of FIDNet will not be evaluated.

2. Factor 2: Past Performance

a. The Government will evaluate the Offeror's technical and management capability by examining the Offeror's past performance, as a prime contractor, on previous information security contracts. Only Past Performance data regarding information security work completed within the last three years (1997-1999) or work that is on-going will be evaluated. The lack of relevant past performance will result in the assignment of a neutral rating (*i.e.*, neither favorable nor unfavorable).

b. The Government will evaluate the offeror's past performance as a prime contractor on Information Security contracts. The evaluation will focus on the offeror's technical understanding and technical capability as demonstrated by the size, scope, complexity and results achieved in the completion of actual tasks similar to those in the Statement of Work. Technically complex tasks implemented and managed across an enterprise will be rated more highly than tasks of less size, scope and complexity. The results achieved in each contract will be an important part of the evaluation of the offeror's technical past performance.

c. The Government will evaluate the Offeror's past performance as the prime contractor in management of large and complex information security efforts as related to the Statement of Work. The evaluation will focus on the management tools and techniques applied to previous efforts and the results achieved. Special emphasis will be placed on the application and use of quality assurance programs with performance metrics.

d. The government will evaluate the offeror’s past performance as it relates to technical expertise and depth of personnel, and the offerors ability to recruit, train, maintain, and retain a high quality Information Security work force.

e. For large businesses, the feasibility and comprehensiveness of the offeror's planned approach to meeting the established subcontracting goals of 10% to small business, 6% to Small Disadvantaged Business/Historically Black Colleges and Universities, and 4% to Small Women Owned Business will be evaluated.

(e) Cost/Price:

1. The offeror is required to submit all pricing data in the format indicated in Sections B and L.

a. The proposed prices in Section B will be evaluated with respect to their completeness and reasonableness. Offerors must submit prices for the complete set of requirements. The reasonableness of the overall price will

be determined on the basis of adequate price competition and by comparison with the Independent Government Cost Estimate (IGCE).
b. The Government will evaluate the realism of the price proposal with respect to the ability of the offeror to meet requirements in terms of skills required, complexity of disciplines and job difficulty only if the Government deems such analysis is necessary. Offeror's price proposals may be compared to the technical proposal to determine the offeror's (1) understanding of work to be performed and (2) capability and capacity to perform the required work and provide the required service. Unrealistically low prices may indicate an inability to understand requirements and a high-risk approach to contract performance and the ability to attract and maintain a high quality workforce. Accordingly, the Government may consider the findings of such an analysis in evaluating an offeror's ability to perform and the risk of its approach.

(2). The price evaluation will be based on the total bottom line price for each proposal.

a. The total bottom line price will be determined based on the proposed prices for the line items and quantities shown in the price tables in Section B. The evaluation will cover a 60-month service period. The line items and quantities listed in Section B are for evaluation purposes only. Actual quantities shall be ordered by subscribing agencies and may vary upwards or downwards from those specified.

b. Offerors are required to submit their proposed prices for the entire 60-month period in the Cost Model. The evaluation period commences with the date of contract award and ends 60 months later. Contract months and evaluation months are assumed to be one and the same.